УДК 004.056 **DOI** 10.15622/ia.25.1.3

В.М. Крундышев, М.О. Калинин

ОЦЕНКА ЭФФЕКТИВНОСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМАХ УМНОГО ГОРОДА НА ОСНОВЕ МОДЕЛИ КОНКУРЕНЦИИ

Крундышев В.М., Калинин М.О. **Оценка эффективности обеспечения информационной безопасности в системах умного города на основе модели конкуренции.**

Аннотация. Реализация концепции умного города (smart city) подразумевает переход от традиционных компьютерных сетей, имеющих четкий информационный периметр, к распределенным сетям нового поколения. Для распределенных подсистем умного города свойственны реконфигурируемая сетевая топологии, открытость, мобильность узлов и построение защиты информации на базе распределенных реестров данных, что открывает новые возможности для злоумышленников. Ситуация осложняется тем, что скорость создания новых цифровых инфраструктур превосходит скорость разработки средств защиты, отвечающих актуальным вызовам. Учитывая специфические свойства объекта защиты, динамику развития угроз безопасности и ограниченный выбор защитных механизмов, для поддержания высокого уровня защищенности систем умного города необходимо проводить непрерывную оценку эффективности защиты и ее перенастройку. В результате анализа существующих решений по оценке эффективности систем обеспечения информационной безопасности установлено, что они работают в проактивном режиме и не учитывают высокую динамику системы «угрозы-защиты» в системах умного города. В статье представлена построенная модель оценки эффективности обеспечения информационной безопасности, базирующая на нелинейной динамической модели конкуренции за влияние на функционирование информационной инфраструктуры. Для поддержания устойчивого состояния системы умного города необходимо выполнение критерия о соотношении скоростей обнаружения и развития компьютерной атаки в инфраструктуре. На разработанном экспериментальном макете эмулированы сценарии развития компьютерных атак «эксплуатация уязвимости ПО», «распределенный отказ в обслуживании», «черная дыра» и «атака большинства» на примере интеллектуальной транспортной сети VANET в инфраструктуре умного города при использовании различных конфигураций системы защиты. В ходе сравнительного эксперимента разных конфигураций системы защиты сети VANET показано, что пример комплекса, реализующего обнаружение атак с помощью сверточной нейросети, динамическую маршрутизацию на базе муравьиного алгоритма и протокол Hashgraph с внедренной моделью доверия, удовлетворяет критерию устойчивости. Применение предложенной модели оценки позволяет обоснованно контролировать и динамически регулировать конфигурацию системы защиты.

Ключевые слова: критерий устойчивости, модель конкуренции, оценка эффективности, распределенный реестр, скорость развития компьютерной атаки, точка устойчивости, умный город.

1. Введение.

В последние годы внимание специалистов из разных отраслей экономики приковано к развивающейся технологической концепции умного города (от англ. «smart city»), предполагающей объединение всех основных жизненно важных

подсистем городского хозяйства (ЖКХ, транспорт, медицина, экология, обеспечение правопорядка, водо- и энергоснабжение и пр.) в единую цифровую экосистему [1 – 3]. Согласно расчетам аналитиков McKinsey, к 2030 году умные города будут генерировать почти 70% мирового ВВП [4]. Технологическим базисом подсистем умного города являются компьютерные сети нового поколения, включая Интернет вещей (IoT), сенсорные сети (WSN), сети транспортных средств (VANET) и прочие динамически реконфигурируемые сети устройств, а также системы распределенного реестра, применяемые для организации контролируемого и верифицируемого обмена данными между участниками сети умного города [5 – 8].

Для обеспечения информационной безопасности систем, имеющих постоянную инфраструктуру и четкий периметр, традиционно применяется стандартный перечень средств защиты, таких как межсетевые экраны, антивирусные программы, SIEM- и DLP-системы. На рынке существует ряд решений, предлагаемых крупными производителями и подтвердивших свою эффективность при обнаружении компьютерных атак типа «отказ в обслуживании», при блокировке вредоносных программ, фильтрации фишинговых сообщений и спама. Ведущие компании в области разработки средств защиты десятилетиями накапливали опыт, получая обратную связь от пользователей, и дорабатывали свои решения, делая их более функциональными, эффективными и универсальными. Основными же свойствами систем умного города являются их динамика и неоднородность, что затрудняет применение традиционных методов и средств защиты информации [8 – 10]. Ситуация осложняется тем, что скорость внедрения систем умного города превышает скорость разработки специализированных средств защиты для них, чем активно пользуются злоумышленники. Отсутствие статического периметра защиты, самоорганизация мобильных узлов в отдельные сегменты, децентрализованное хранение больших объемов данных, возможность перемещения узлов сети – все это открывает новые возможности как для прогресса технологий умных городов, так и для нарушителей безопасности, которые реализуют специфические компьютерные атаки, направленные на нарушение устойчивого функционирования систем умных городов и эксплуатирующие новые уязвимости (например, в динамической маршрутизации и в распределенном реестре) [11 – 14].

В таких условиях одной из ключевых проблем является оценка эффективности обеспечения информационной безопасности в системах умного города. Нечеткость структуры объекта защиты и внедрение

новых компьютерных технологий приводит к тому, что формирование единых подходов к построению системы защиты цифровых инфраструктур умного города становится невозможным. С учетом постоянных изменений, происходящих в объекте защиты, и постоянно меняющегося ландшафта угроз безопасности необходимо регулярно проверять адекватность системы обеспечения информационной безопасности умного города с целью выявления ее слабых мест и соответствующей перенастройки защитных механизмов. Для решения поставленной задачи в статье рассматриваются следующие аспекты:

- представлены результаты анализа существующих подходов к оценке эффективности обеспечения информационной безопасности, а также определены требования, которым должна отвечать разрабатываемая модель оценки с учетом характерных особенностей систем умного города;
- для оценки эффективности обеспечения информационной безопасности предложена динамическая модель конкуренции, описывающая взаимодействие разных видов узлов: легитимных узлов и узлов-нарушителей в изменяющейся среде умного города. В данной модели отражается постоянная конкуренция узлов за ресурсы, то есть за характеристики системы умного города, что приводит к эволюционным изменениям в системе;
- на базе сетевого эмулятора разработан экспериментальный макет, поддерживающий модель системы умного города и различные тестовые сценарии компьютерных атак, на котором проведена экспериментальная оценка предложенного решения.

2. Анализ подходов к оценке эффективности систем обеспечения информационной безопасности. В настоящее время выделяются следующие основные подходы к оценке эффективности обеспечения информационной безопасности:

1. Экспертный. Данный подход предполагает использование опыта и знаний экспертов, специализирующихся на защите объектов информатизации. Штатные сотрудники/приглашенные специалисты на основе анализа имеющихся данных принимают решения по оценке эффективности применяемых защитных механизмов. Так, например, в работе [15] представлена экспертная система оценки уровня соответствия системы защиты предъявляемых требованиям. Авторы выделяют три основных этапа: подготовка исходных данных, контроль реализации требований и вычисление итоговых показателей оценки обеспечения информационной безопасности. В работе [16] предложен подход к оценке эффективности, основанный на использовании метода экспертных оценок, в котором полученные показатели уровня

защищенности помогают эксперту определиться с принятием правильного решения по рассматриваемым мерам обеспечения безопасности. Преимуществом экспертного подхода является гибкость и высокий экспертный уровень принятых решений. Недостаток заключается в том, что точность оценки зависит от квалификации экспертов. Кроме того, такой подход не позволяет реализовать непрерывную объективную оценку.

2. Статистический. Данный подход предполагает определение показателя эффективности на основе статистических данных. Как правило, оценка эффективности вычисляется с использованием статистических мер, например, таких как среднее, среднеквадратичное отклонение, коэффициент корреляции, для сравнения расчетных и измеренных значений. Например, в статье [17] представлена методика оценки эффективности системы защиты, основанная на стохастическом представлении деструктивных воздействий и процесса ликвидации их последствий. Преимуществом данного подхода является высокая точность оценки эффективности в условиях нехватки данных о текущем состоянии информационной инфраструктуры. Недостатком является то, что точность полученной оценки напрямую зависит от объема имеющихся данных.

3. Вероятностный. Данный подход предполагает использование вероятностных моделей и критериев. В ряде случаев задаются диапазоны значений с определенными вероятностями их наступления. Например, в исследовании [18] представлена модель оценки показателя эффективности обеспечения информационной безопасности, базирующаяся на использовании операционного метода преобразования Лапласа и численного метода решения системы линейных алгебраических уравнений методом Гивенса. В работе [19] построена методика оценивания результативности системы обнаружения веб-бэкдоров, основанная на расчете трех групп частных показателей, характеризующих действенность, ресурсоемкость и оперативность работы системы обнаружения, а также вычислении обобщенного показателя результативности. В исследовании [20] представлена методика оценивания вероятности безотказной работы систем защиты информации от несанкционированного доступа при обеспечении конфиденциальности информации на базе метода эквивалентных схем. Преимущество данного подхода заключается в низкой вероятности ошибок, связанных с субъективными оценками. Недостатком является то, что вероятностные модели могут устареть и перестать быть актуальными в результате изменений информационной инфраструктуры и систем защиты.

4. Нейросетевой. Данный подход предполагает обучение вычислительной модели машинного обучения на наборе данных, содержащем информацию о параметрах объекта защиты, действующих угрозах безопасности и конфигурации системы защиты. В результате обучения на этапе эксплуатации нейросетевая модель может принимать решения о выборе оптимальной конфигурации средств защиты информации. Например, в работах [21, 22] представлен алгоритм модели оценки защищенности информационной системы на основе нейросети. Для обучения нейросети используется алгоритм обратного распространения ошибки. Преимущество нейросетевого подхода заключается в возможности обнаружения скрытых закономерностей в данных. Недостатком является то, что точность оценки эффективности средств защиты напрямую зависит от обучающего набора данных, в результате чего такое решение требует значительных временных затрат на внедрение и калибровку.

5. На основе нечеткой логики. Данный подход предполагает применение аппарата нечеткой логики для описания текущего состояния объекта защиты, системы обеспечения информационной безопасности и действующих киберугроз. В условиях неопределенности динамически меняющиеся параметры описываются в виде нечетких переменных, также определяется функция принадлежности. Например, в исследовании [23] для оценки уровня защищенности использован аппарат нечеткой логики, а для оценки стойкости элементов защиты введены и использованы нечеткие переменные «вероятность появления угрозы», «величина ущерба», «степень сопротивляемости». В работах [24, 25] представлены похожие методики оценки эффективности системы зашиты распределенных информационных систем, базирующаяся на нечеткой продукционной системе с установленными в результате экспериментов оптимальными параметрами и алгоритмом нечеткого вывода. Преимущество данного подхода заключается в том, что он не требует наличия точной и полной информации. Недостатком является то, что для высокой точности оценки эффективности защиты необходимо предварительно с привлечением экспертов подготовить базу знаний, определив терм-множества и диапазоны.

6. Комбинированный. Предполагается использование ансамбля различных эвристик и алгоритмов для оценки эффективности конфигурации системы защиты и поиска оптимального решения. В ряде случаев для решения задачи оптимизации применяются биоинспирированные методы. Например, в исследовании [26] применяется генетический алгоритм для выбора

оптимальной конфигурации системы защиты информации с учетом изменяющихся условий среды, уровня профессиональной подготовки работников, количества отказов в работе оборудования и скорости развития компьютерной атаки. В работе [27] авторы исследуют применимость гибридного подхода к оперативной оценке защищенности критически важных ресурсов, сочетающего традиционные методы фильтрации Калмана с возможностями искусственных нейросетей. Преимущество комбинированного подхода заключается в его гибкости. Недостатком является высокая сложность вычислений и подбора параметров алгоритма при больших объемах анализируемых данных.

7. Графовый (с использованием методов теории графов). Данный подход предполагает представление информационной инфраструктуры в виде графа, где узлы (вершины) графа представляют собой компоненты системы (например, серверы, устройства, процессы), а ребра графа представляют собой связи между этими компонентами (например, сетевые соединения, зависимости между программными модулями). Математическая модель, представленная в виде набора графов, позволяет описывать и анализировать системы и движение информационных активов и потоков предприятия, их взаимовлияния с целью выявления потенциальных угроз информационной безопасности и оценки эффективности спроектированной системы защиты информации. Например, в исследовании [28] представлен подход к оценке эффективности обеспечения информационной безопасности на основе построения и анализа дерева атак, состоящем из программно-технических атак (направленных на объекты информационной инфраструктуры) и социоинженерных атак (направленных на санкционированных пользователей). В работе [29] представлена динамическая система защиты, состоящая из взаимодействующих подсистем обеспечения безопасности, поддерживающих возможность переключения компонентов внутри одной подсистемы. В статье [30] рассмотрен метод повышения эффективности управления защитой, в основе которого лежит вычисление комплексного показателя защищенности, а также построение графа защищенности, учитывающего реальную структуру компьютерной сети и системы защиты информации. Преимущество графового подхода заключается в том, что он позволяет представить сложную сетевую инфраструктуру в виде наглядной модели, что упрощает понимание топологии сети и связей ее элементов. Недостатком является то, что точность оценки защищенности при использовании данного подхода определяется

непротиворечивостью и качеством входных данных, которые используются для построения графа, а также необходимостью специальных алгоритмов обработки знаний, представленных в виде графов.

8. На основе моделирования состояний системы. Данный подход позволяет анализировать последовательность событий и вероятности переходов между состояниями безопасности, что помогает оценить эффективность мер защиты и выявить слабые места. Защищаемую информационную инфраструктуру можно представить как систему, находящуюся в различных состояниях (например, «защищена», «атакована», «скомпрометирована», «восстановлена»). Например, в исследовании [31] представлена математическая модель, в основу которой положен аппарат сетей Петри-Маркова, получены аналитические соотношения для расчета предложенного показателя на примере жизненного цикла входящих электронных документов с учетом времени выполнения типовых процедур и функций их обработки, времени реализации угроз, а также применения мер защиты. В работе [32] для выбора оптимального набора средств защиты от компьютерных атак использован аппарат поглощающих цепей Маркова. Решаемая задача была сведена к максимизации среднего времени до отказа безопасности при ограничениях на стоимость набора защитных механизмов. Преимущество данного подхода заключается в том, что он позволяет работать с трассой состояний системы и оценивать эффективность защиты в перспективе. Недостатком является то, что подход подразумевает упрощение реальной системы, в результате чего не все факторы, влияющие на ее безопасность, учитываются.

Результаты анализа подходов к оценке эффективности систем обеспечения информационной безопасности представлены в таблице 1.

Таким образом, в результате анализа известных подходов к оценке эффективности систем обеспечения информационной безопасности можно сделать вывод, что большинство рассмотренных решений требуют наличия точных исходных данных об объекте защиты, действующих угрозах безопасности и доступных механизмах защиты. Однако, в быстроменяющихся условиях умного города исходные данные быстро теряют свою актуальность и перестают отражать фактическое состояние системы. В таких условиях наиболее перспективными являются решения, базирующиеся на математических моделях, характеризующих динамику изменений как объекта защиты, так и действующих угроз.

Таблица 1. Результаты анализа подходов

Подход	Особенности	Преимущества	Недостатки
Экспертный	Использование опыта и знаний экспертов	Гибкость и высокий экспертный уровень принятых решений	Точность оценки зависит от квалификации экспертов
Статистический	Определение показателя эффективности на основе статистических данных	Высокая точность оценки эффективности в условиях нехватки данных о текущем состоянии информационной инфраструктуры	Точность оценки зависит от объема имеющихся данных
Вероятностный	Использование вероятностных моделей и критериев	Низкая вероятности ошибок, связанных с субъективными оценками	Риск устаревания вероятностной модели
Нейросетевой	Обучение модели на наборе данных, содержащем информацию о параметрах объекта защиты, действующих угрозах безопасности и конфигурации системы защиты	Возможность обнаружения скрытых закономерностей в данных	Временные затраты на внедрение и калибровку нейросетевой модели
На основе нечеткой логики	Применение аппарата нечеткой логики для описания текущего состояния объекта защиты, системы обеспечения информационной безопасности и действующих киберугроз	Не требует наличия точной и полной информации	Необходимость привлечения экспертов для подготовки базы знаний, определения терм-множеств и диапазонов
Комбинированный	Использование ансамбля различных эвристик и алгоритмов для оценки эффективности конфигурации системы защиты и поиска оптимального решения	Гибкость	Высокая сложность вычислений и подбора параметров алгоритма при больших объемах анализируемых данных
Графовый	Представление информационной инфраструктуры в виде графа, где узлы графа представляют собой компоненты системы, а ребра графа представляют собой связи между этими компонентами	Представление сложной сетевой инфраструктуры в виде наглядной модели	Необходимость использования специальных алгоритмов обработки знаний, представленных в виде графов
На основе моделирования состояний системы	Анализ последовательности событий и вероятности переходов между состояниями безопасности	Работа с трассой состояний системы и оценка эффективности защиты в перспективе	Упрощение реальной системы

Применение методов теории графов и цепей Маркова для описания состояний объекта защиты и системы обеспечения информационной безопасности ограничено необходимостью ввода в реальную систему дополнительного параметра – временного лага между моментом, когда действие осуществляется, и моментом, когда наблюдается его эффект. Учитывая сказанное, для оценки эффективности защиты предлагается разработать динамическую модель без временных задержек, на вход которой подается минимальный объем данных. В рамках исследования предлагается свести задачу оценки эффективности обеспечения информационной безопасности в системах умного города к задаче поиска оптимального решения при ограниченном выборе механизмов защиты.

3. Динамическая модель конкуренции. Учитывая особенности систем умного города, а также наличие в сети двух типов узлов (легитимных узлов и узлов-нарушителей), предлагается провести аналогию с нелинейными динамическими моделями взаимодействия двух конкурирующих видов, применяемых в экологии и других смежных областях науки.

Традиционные природоподобные модели (модели конкуренции видов) без временных задержек состоят из системы дифференциальных уравнений, характеризующих популяцию видов в каждый момент времени [33, 34]. Классическая модель конкуренции, предложенная А.Лоткой и В.Вольтеррой [35], описывается системой дифференциальных уравнений вида (1):

$$\begin{cases} \frac{dx}{dt} = (\alpha - \beta y)x \\ \frac{dy}{dt} = (\delta x - \gamma)y \end{cases}, \quad (1)$$

где x и y – зависимости от времени t, которые характеризуют соответственно, количества видов жертв и хищников; α – вероятность того, что жертвы размножатся; γ – вероятность того, что хищник умрет от голода; β – вероятность того, что жертва будет съедена хищником; δ – вероятность того, что хищнику хватит еды на дальнейшее размножение.

Как правило, для решения прикладных задач применяются модификации классической модели «хищник-жертва». Расширение возможностей классической модели «хищник-жертва» осуществляется путем добавления ограничений на количество ресурсов для жертв, учета влияния окружающей среды, создания пространственной

структуры, а также за счет ввода нескольких видов жертв и хищников [36 – 38]. Так, расширенные модели конкуренции успешно применяются в экологии и медицине. Например, в исследовании [39] рассмотрена возможность применения модели «хищник-жертва» для моделирования процессов, связанных с очисткой сточных вод, где загрязнитель вступает в качестве жертвы, а биологически активный ил – в роли хищника. В исследовании [40] представлена медицинская модель иммунной реакции, в рамках которой описывается взаимодействие между антигеном и антителом. Также, модель конкуренции применяется в компьютерных науках для описания динамики взаимодействия между различными узлами в компьютерной сети, для моделирования процессов, борющихся за обладание ресурсами (например, несколько процессов могут конкурировать за процессорное время или за память), а также в сценариях информационной безопасности, где в роли жертвы выступает сценарий инцидента, а в роли хищника – защитный механизм [41]. Таким образом, учитывая имеющийся успешный опыт применения моделей конкуренции в различных областях, в том числе в компьютерных науках, предлагается применить модель конкуренции без временных задержек для описания взаимодействия компонентов систем умного города и последующей оценки эффективности применяемых защитных механизмов.

Расширение исходной модели и добавление дополнительных факторов и закономерностей, описываемых явными функциями, позволит полно отразить динамику системы умного города с учетом наличия в ней нескольких конкурирующих видов. В качестве конкурирующих видов выступают легитимные узлы и узлы-нарушители. При расширении исходной модели также необходимо учитывать, что информационная инфраструктура умного города характеризуется разным уровнем защищенности узлов. В рамках одной компьютерной сети могут взаимодействовать как оснащенные передовыми средствами защиты центральные серверы и базы данных, так и слабо защищенные устройства и датчики Интернета вещей умного города и систем городского хозяйства. Проэксплуатировав уязвимости ПО слабо защищенных устройств, злоумышленник может создать ботнет, который будет использован для реализации компьютерных атак, направленных на вывод из строя центральных серверов и магистрального сетевого оборудования, реализации атаки большинства на системы распределенного реестра и т.д. Учитывая особенности систем умного города и наиболее вероятные сценарии реализации компьютерных атак, при разработке модели оценки

эффективности обеспечения информационной безопасности определены следующие понятия:

– хищник (malicious, *M*) – устройство, которое осуществляет целенаправленные компьютерную атаку на систему умного города, маршрутизацию и отдельные целевые устройства (устройства-жертвы);

– жертва (normal, *N*) – устройство, которое выполняет свою целевую функцию и не осуществляет деструктивных воздействий по отношению к системе умного города;

– инфицированное устройство (zombie, *Z*) – «устройство-зомби», которое осуществляет деструктивное воздействие в отношении системы умного города и находится под управлением злоумышленника;

– вакцинированное устройство (protected, *P*) – устройство, которое в период действия вакцины является более защищенным от атак за счет использования дополнительных средств защиты;

– выведенное из строя устройство (broken, *B*) – устройство, неспособное в полной мере выполнять целевую функцию (в терминах классической модели – мертвая жертва).

Все множество устройств системы умного города представлено в виде совокупности пяти классов: *M* (malicious) и *Z* (zombie) – хищники, *N* (normal), *P* (protected) и *B* (broken) – жертвы (рисунок 1).

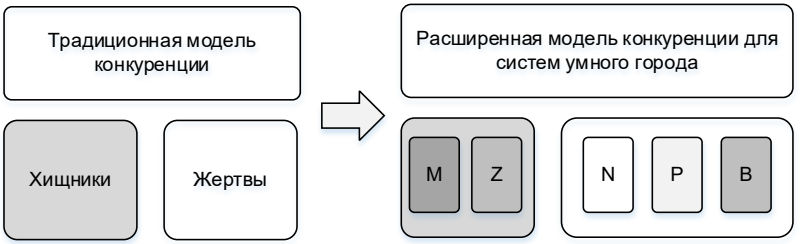

Рис. 1. Классы устройств системы умного города

Устройства классов *N* и *P* успешно выполняют целевую функцию, при этом устройства класса *P* обладают дополнительными механизмами защиты от компьютерных атак (являются вакцинированными). Устройства класса *B* выведены из строя, при этом они не представляют угрозы для других устройств и могут быть либо восстановлены в класс *N*, либо со временем перейти в состояние *D*. Устройства класса *M* находятся под прямым управлением злоумышленников, реализуют компьютерные атаки и стремятся

перевести устройства из классов *P* и *N* в классы *Z* и *B* в зависимости от целей и мотивов. Устройства класса *Z* являются зомби, они реализуют компьютерные атаки на устройства классов *N* и *P*, стремясь перевести их в класс *B*, при этом они могут быть восстановлены в класс *P*. Состояние *D* – терминальное состояние, при котором устройство вышло из строя. Устройства класса *B* переходят в это состояние, если они не были своевременно восстановлены в класс *N*, а устройства классов *M* и *Z* при успешной работе защитных механизмов. На рисунке 2 представлена диаграмма состояний объектов.

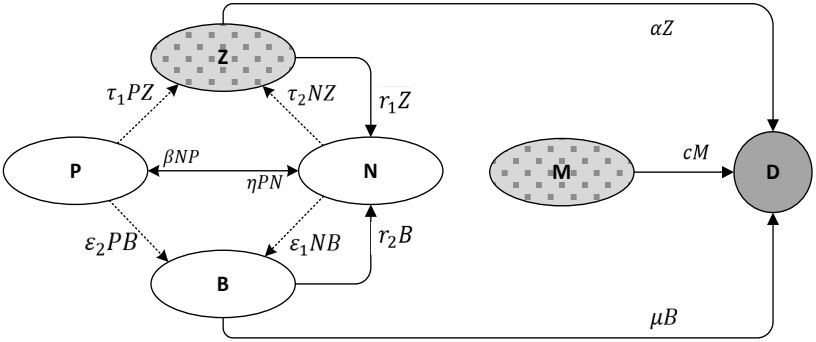

Рис. 2. Диаграмма состояний объектов системы умного города

Устройства классов *Z* и *B* могут быть восстановлены в класс *N* с вероятностями r_1 и r_2. Устройства класса *M* инфицируют устройства *N* и *P* с вероятностями τ_1 и τ_2. Под воздействием устройств из классов *M* и *Z* жертвы из классов *N* и *P* могут перейти в класс *B* с коэффициентами ε_1 и ε_2. μ, a, c – коэффициенты вымирания устройств класса *B*, *Z*, *M*. Устройства класса *N* становятся вакцинированными (переходят в класс *P*) с вероятностью β. Устойчивость к заражению (вакцинация) пропадает со скоростью, прямо пропорциональной коэффициенту η. Устройства классов *Z* и *M* могут вымирать только под воздействием системы защиты – «охотника», которая напрямую влияет на значение коэффициентов a и c. Вероятностные коэффициенты модели определяются на основе статистических данных за прошедший период, а также в результате экспертной оценки. Коэффициенты модели указаны в таблице 2.

Таблица 2. Коэффициенты модели

	N	***P***	***B***	***Z***	***M***	***D***
N		β	ε_1	τ_2		
P	η		ε_2	τ_1		
B	r_2					μ
Z	r_1					a
M						c
D						

Исходя из введенных обозначений и модели конкуренции, формальное описание состояний системы умного города и развития компьютерных атак в ней можно представить в виде системы (2):

$$\begin{aligned}
\frac{dN}{dt} &= n_g N\left(1-\frac{N}{Q_N}\right) + NP(\eta-\beta) - \varepsilon_1 NB - \tau_2 NZ + r_2 B + r_1 Z - m_N N \\
\frac{dP}{dt} &= p_g P\left(1-\frac{P}{Q_P}\right) + NP(\beta-\eta) - \varepsilon_2 PB - \tau_1 PZ - m_P P \\
\frac{dB}{dt} &= b_g B\left(1-\frac{B}{Q_B}\right) + \varepsilon_1 NB + \varepsilon_2 PB - r_2 B - B(\mu + m_B) \\
\frac{dZ}{dt} &= z_g Z\left(1-\frac{Z}{Q_Z}\right) + \tau_2 NZ + \tau_1 PZ - r_1 Z - aZ \\
\frac{dM}{dt} &= m_g M\left(1-\frac{M}{Q_M}\right) - cM
\end{aligned} \quad . \qquad (2)$$

В системе уравнений параметры Q_N, Q_P, Q_B, Q_Z, Q_M отражают количество устройств, принадлежащих классам *N*, *P*, *B*, *Z*, *M*, соответственно. Коэффициенты n_g, p_g, b_g, z_g, m_g характеризуют рост количества устройств в классах *N*, *P*, *B*, *Z*, *M*, соответственно. Параметры m_P, m_B, m_N отражают вероятность промаха «охотника» (попадания по устройствам из классов *P*, *B*, *N*).

4. Формализация решаемой задачи. Определение критерия устойчивости. Согласно предложенной модели, решаемой задачей является максимизация коэффициентов вымирания для классов *M* и *Z*, при этом вероятности промаха должны стремиться к нулю (3). Кроме того, учитывая, что устройства класса *Z* могут быть восстановлены в класс *N*, относительно класса *Z* введен коэффициент r_1, который наравне с a, должен стремиться к максимуму:

$$\begin{cases} \begin{cases} m_N \to 0 \\ m_P \to 0 \\ m_B \to 0 \end{cases} \\ \begin{bmatrix} r_1 \to \infty \\ a \to \infty \end{bmatrix} \\ c \to \infty \end{cases}. \quad (3)$$

Для оценки эффективности обеспечения безопасности систем умного города в условиях воздействия актуальных угроз безопасности определена точка устойчивости системы – идеал.

Идеалом системы (2) является состояние, при котором в модели присутствуют устройства классов *N* и *P*, выполняющие свою целевую функцию, а устройства классов *M*, *Z* и *B* отсутствуют.

Точка устойчивости системы $P_0(N_0, P_0, B_0, M_0, Z_0) = P_0(N_0, P_0, 0, 0, 0)$ достижима при значениях (4):

$$\begin{cases} N_0 = Q_N + \dfrac{Q_N(Q_P p_g n_g - Q_P Q_N(\eta - \beta)(n_g - m_N) - m_P Q_P n_g)(\eta - \beta)}{p_g {n_g}^2 + n_g Q_P Q_N(\eta - \beta)^2} - \dfrac{Q_N m_N}{w_g} \\ P_0 = \dfrac{Q_P p_g n_g - Q_P Q_N(\eta - \beta)(n_g - m_n) - m_P Q_P n_g}{p_g n_g + Q_P Q_N(\eta - \beta)^2} \\ B_0 = 0 \\ M_0 = 0 \\ Z_0 = 0 \end{cases}. \quad (4)$$

Тогда для достижения точки устойчивости необходимо решить задачу оптимизации функции «охотника» (5):

$$h_\Phi(t) \to max. \quad (5)$$

Функция $h_\Phi(t)$ имеет динамический параметр $\Phi = \{\varphi_1, \dots, \varphi_n\}$, который представляет собой исследуемый в данный момент времени t набор входных данных: параметры системы умного города, доступные вычислительные ресурсы, текущий уровень угроз безопасности. На основе входных данных $\{\Phi_0, t_0\}$ функция $h_\Phi(t)$ определяет, какой из защитных механизмов должен быть выбран для обеспечения наиболее точного и быстрого анализа угроз и реагирования на них.

Критерием устойчивости защищаемой системы служит совокупность условий (6) (скорость вымирания устройств-злоумышленников и устройств-зомби выше, чем скорость перехода устройств из нормального состояния в зараженное или выведенное из строя, при этом количество ложных срабатываний не должно превышать λ, при $Q_M > 0$ и $Q_Z > 0$):

$$\begin{cases} m_N \leq \lambda \\ m_P \leq \lambda \\ m_B \leq \lambda \\ a > \varepsilon_1 \\ a > \varepsilon_2 \\ a > \tau_1 . \\ a > \tau_2 \\ c > \varepsilon_1 \\ c > \varepsilon_2 \\ c > \tau_1 \\ c > \tau_2 \end{cases} \quad (6)$$

Таким образом, в соответствии с разработанной моделью эффективная защита должна обеспечить выполнение системы (6).

5. Экспериментальное исследование. На базе сетевого эмулятора NS-3 разработан экспериментальный макет, включающий имитационные модели типовых систем умного города: сеть транспортных средств (сеть VANET), промышленный интернет вещей (IIoT) и сервис управления энергоресурсами. При запуске сценария пользователю необходимо указать ряд параметров: город, общее количество узлов в сети, плотность расположения придорожной инфраструктуры (базовых станций, умных светофоров, электронных табло, АЗС и т.д.) и транспортных средств, максимальную скорость движения автомобилей, протокол маршрутизации сетевого трафика (реактивный AODV или проактивный OLSR). Также необходимо установить параметры моделирования компьютерных атак (указав тип атаки, время начала и окончания атаки, количество узлов-злоумышленников). Далее в зависимости от выбранных параметров запускается определенный сценарий моделирования, наблюдать за ходом моделирования можно с использованием визуализатора NetAnim. В процессе моделирования генерируются синтетические данные трех типов: дамп сетевого трафика, таблицы маршрутизации и общая статистика о состоянии системы умного города (текущая пропускная способность, количество доставленных и потерянных сетевых пакетов и т.д.).

На рисунке 3 представлен пример экспериментального сценария, в котором злоумышленник последовательно реализует компьютерные атаки на динамическую маршрутизацию и систему распределенного реестра, используемые в сети транспортных средств VANET. Данный сценарий предполагает сетевое взаимодействие

узлов-автомобилей и объектов придорожной инфраструктуры умного города.

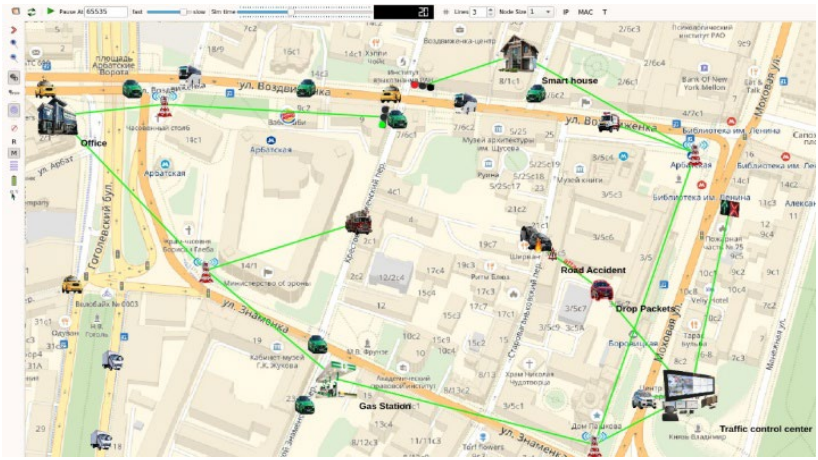

Рис. 3. Моделирование «атаки большинства» на распределенный реестр в сети транспортных средств (VANET) умного города

В ходе рассматриваемого сценария два автомобиля попадают в ДТП, после чего производят попытку отправить соответствующее сообщение в центр управления дорожным движением. Злоумышленник реализует классическую атаку «черная дыра» (blackhole attack) [42], направленную на нарушение маршрутизации между узлами, в результате чего отбрасываются сетевые пакеты, полученные от автомобилей, попавших в ДТП, и вследствие этого спасательные службы не получают сообщение об автомобильной аварии и не прибывают на место происшествия. Далее нарушитель безопасности реализует известную «атаку большинства» (majority attack, 51% attack) [43], нацеленную на используемый в системе распределенный реестр. Атака большинства возникает, когда злоумышленник (группа злоумышленников) получает контроль над более чем 50% вычислительной мощности сети реестра, что позволяет манипулировать консенсусом – в таком случае атакующий может проводить двойное расходование средств, исключать транзакции и изменять порядок транзакций, а также нарушать работу сети, подрывая ее децентрализованность и доверие со стороны пользователей. В рассматриваемом сценарии успешная атака большинства ставит под угрозу целостность распределенного реестра, в результате чего приостанавливается подтверждение новых транзакций, и, как

следствие, пострадавшая сторона не получает страховую выплату от страховой компании за произошедшее ДТП.

Система защиты, состоящая из набора детекторов, реализована в виде отдельного программного модуля. Для обнаружения вредоносной активности используются как традиционные эвристические, пороговые и сигнатуры методы защиты (эксперимент 1), так и современные средства – обнаружение атак с помощью сверточной нейросети, динамическую маршрутизацию на базе муравьиного алгоритма и протокол блокчейна Hashgraph с внедренной моделью доверия (эксперимент 2). На вход системе в режиме реального времени подаются сгенерированные в ходе моделирования синтетические данные. На основе анализа полученных данных системой принимается решение об обнаружении и блокировке узла-нарушителя. Также непрерывно работает программный модуль, реализующий созданную модель оценки эффективности системы защиты. В ходе моделирования непрерывно ведется оценка количества узлов разных типов.

Для рассматриваемого демосценария на рисунках 4 и 5 показана запротоколированная динамика количества узлов каждого класса под воздействием компьютерных атак «черная дыра» (начало в точке 40 сек.) и «атака большинства» (начало в точке 220 сек.).

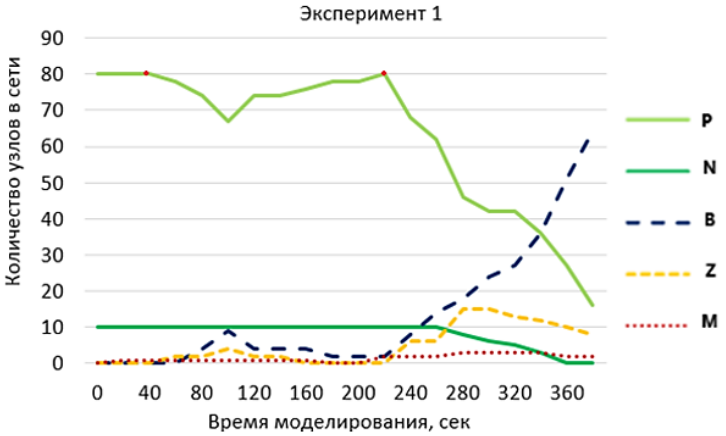

Рис. 4. Динамика количества узлов (эксперимент 1)

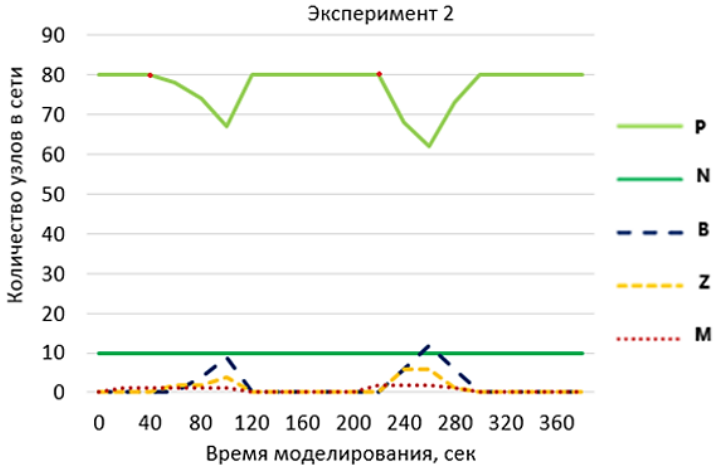

Рис. 5. Динамика количества узлов (эксперимент 2)

Система обеспечения информационной безопасности, использованная в первом эксперименте (рисунок 4), не соответствует установленному критерию устойчивости. При первой атаке в точке, соответствующей отсчету времени 40 сек., нарушитель своевременно обнаружен и изолирован, в результате чего маршрутизация сетевого трафика восстанавливается ко времени 220 сек. Однако, вторая компьютерная атака обнаружена слишком поздно, что привело к нарушению целостности распределенного реестра и остановке транзакций. В ходе альтернативного сценария (рисунок 5) система защиты с адаптированной конфигурацией детекторов своевременно обнаружила обе атаки и изолировала узлы-нарушителей, в результате чего сеть VANET вернулась в рабочее состояние.

Для проведения более масштабного эксперимента разработан сценарий, в котором злоумышленник последовательно реализует серию компьютерных атак на информационную инфраструктуру умного города. Первая атака – получение контроля над слабозащищенными устройства умного города за счет эксплуатации уязвимости ПО. Вторая атака – распределенная атака типа «отказ в обслуживании» (DDoS-атака) на центральные узлы сети. При реализации данной атаки злоумышленник использует взломанные в ходе первой атаки узлы-зомби. Третья атака – атака «черная дыра», направленная на нарушение маршрутизации сетевого трафика и, как следствие, нарушение стабильной работы сетевого оборудования (базовых станций, коммутаторов и маршрутизаторов). Четвертая

атака – «атака большинства», направленная на нарушение работы системы распределенного реестра. В результате проведения данных атак функционирование сети умного города будет полностью остановлено.

В качестве защитных механизмов реализованы различные методы, предложенные в предыдущих работах авторов. Так, для обнаружения вредоносных сигнатур, предназначенных для взлома слабозащищенных устройств умного города, и обнаружения DDoS-атаки реализован метод на основе сверточной нейросети (в таблице 2 – *CNN*) [44]. Преимуществом данного решения является возможность быстрого анализа больших объемов сетевого трафика. Для обнаружения атаки типа «черная дыра» использованы методы на основе роевого интеллекта: муравьиного алгоритма (в таблице 2 – *Ant*) и капель воды (в таблице 2 – *Wat*) [45]. Преимуществом данного решения является его применимость на узлах с низкой вычислительной мощностью и в условиях централизованности сети, что характерно для инфраструктур умного города. Для обнаружения «атаки большинства» реализован механизм консенсуса на базе протокола Hashgraph, дополненный моделью доверия (в таблице 2 – *Hash*) [46]. Преимуществом данного защитного механизма является возможность выявления и изоляции вредоносных узлов на ранних этапах работы сети, снижая их влияние на процесс голосования и тем самым повышая византийскую отказоустойчивость распределенного реестра, а также устойчивость системы.

В ходе экспериментов тестировались различные комбинации защитных механизмов, включая традиционный подход, в котором используется сигнатурный детектор атак, и переборные сочетания альтернативных защитных механизмов. В таблице 2 представлены результаты оценки эффективности тестовых конфигураций защиты, полученные с использованием разработанной модели. Количество ложных срабатываний не должно превышать λ=0,03 (3%). В соответствии с введенным критерием устойчивости (6) символ «–» означает, что в данный момент в сети нет узлов того типа, для которого рассчитывается коэффициент (например, при реализации первой атаки, целью которой является эксплуатация уязвимости ПО, в сети нет узлов-зомби и узлов, выведенных из строя). Красным цветом и перечеркнутыми знаками сравнения отмечены те условия из критерия (6), которые не выполняются.

В результате сравнительного анализа разных конфигураций установлено, что система защиты, состоящая из набора «сверточная нейросеть + муравьиный алгоритм + протокол Hashgraph,

дополненный моделью доверия», соответствует заданному критерию устойчивости. Данная конфигурация системы защиты может быть результативно использована для защиты сети умного города.

Таблица 2. Сравнительная оценка эффективности различных конфигураций системы защиты

Комбинация средств защиты	**Экспл. уязв. ПО**	**DDoS-атака**	**Атака «черная дыра»**	**Атака большинства**
Традиционный детектор атак на базе контроля сигнатур	$0{,}05 \not\leq 0{,}03$ $0{,}04 \not\leq 0{,}03$ – – – – – $0{,}34 > 0$ $0{,}34 > 0$ $0{,}34 \not> 0{,}53$ $0{,}34 > 0{,}23$	$0{,}02 \leq 0{,}03$ $0{,}02 \leq 0{,}03$ $0 \leq 0{,}03$ $0{,}21 \not> 0{,}52$ $0{,}21 \not> 0{,}42$ $0{,}21 \not> 0$ $0{,}21 \not> 0$ $0{,}36 \not> 0{,}52$ $0{,}36 \not> 0{,}42$ $0{,}36 > 0$ $0{,}36 > 0$	$0{,}24 \not\leq 0{,}03$ $0{,}17 \not\leq 0{,}03$ $0{,}22 \not\leq 0{,}03$ – – – – $0{,}21 > 0$ $0{,}21 > 0$ $0{,}21 > 0$ $0{,}21 > 0$	$0{,}36 \not\leq 0{,}03$ $0{,}31 \not\leq 0{,}03$ $0{,}27 \not\leq 0{,}03$ – – – – $0{,}12 > 0$ $0{,}12 > 0$ $0{,}12 > 0$ $0{,}12 > 0$
…	…	…	…	…
CNN + Ant + Hash	$0{,}01 \leq 0{,}03$ $0{,}01 \leq 0{,}03$ – – – – – $0{,}47 > 0$ $0{,}47 > 0$ $0{,}47 > 0{,}22$ $0{,}47 > 0{,}11$	$0{,}02 \leq 0{,}03$ $0{,}02 \leq 0{,}03$ $0 \leq 0{,}03$ $0{,}44 > 0{,}31$ $0{,}44 > 0{,}21$ $0{,}44 > 0$ $0{,}44 > 0$ $0{,}44 > 0{,}31$ $0{,}44 > 0{,}21$ $0{,}44 > 0$ $0{,}44 > 0$	$0{,}01 \leq 0{,}03$ $0{,}01 \leq 0{,}03$ $0 \leq 0{,}03$ – – – – $0{,}48 > 0$ $0{,}48 > 0$ $0{,}48 > 0$ $0{,}48 > 0$	$0 \leq 0{,}03$ $0 \leq 0{,}03$ $0 \leq 0{,}03$ – – – – $0{,}65 > 0$ $0{,}65 > 0$ $0{,}65 > 0$ $0{,}65 > 0$
…	…	…	…	…
CNN + Wat + PoS	$0{,}01 \leq 0{,}03$ $0{,}01 \leq 0{,}03$ – – – – – $0{,}47 > 0$ $0{,}47 > 0$ $0{,}47 > 0{,}22$ $0{,}47 > 0{,}11$	$0{,}02 \leq 0{,}03$ $0{,}02 \leq 0{,}03$ $0 \leq 0{,}03$ $0{,}44 > 0{,}31$ $0{,}44 > 0{,}21$ $0{,}44 > 0$ $0{,}44 > 0$ $0{,}44 > 0{,}31$ $0{,}44 > 0{,}21$ $0{,}44 > 0$ $0{,}44 > 0$	$0{,}04 \not\leq 0{,}03$ $0{,}03 \leq 0{,}03$ $0{,}02 \leq 0{,}03$ – – – – $0{,}39 > 0$ $0{,}39 > 0$ $0{,}39 > 0$ $0{,}39 > 0$	$0{,}04 \not\leq 0{,}03$ $0{,}03 \leq 0{,}03$ $0{,}01 \leq 0{,}03$ – – – – $0{,}42 > 0$ $0{,}42 > 0$ $0{,}42 > 0$ $0{,}42 > 0$

Например, для другой конфигурации средств защиты, где используется детектор на базе сверточной нейросети, алгоритм капель воды (*Wat*) и протокол консенсуса PoS, большинство условий критерия также выполняется, однако при обнаружении атаки «черная дыра» и

«атаки большинства» количество ложных срабатываний превышает порог, а скорость вымирания узлов-нарушителей значительно снижается по сравнению с предыдущей рассмотренной конфигурацией.

6. Заключение. Проведенное исследование позволило установить, что оценка эффективности систем защиты умного города должна базироваться на динамических математических моделях, учитывающих эволюцию как объекта защиты – защищаемой инфраструктуры, так и атакующей стороны – объекта угроз. В данном исследовании построена модель оценки эффективности обеспечения информационной безопасности в системах умного города, базирующаяся на модели конкуренции. Разработанная модель демонстрирует, что устойчивость системы достигается при условии преобладания скорости вымирания злоумышленников и устройств-зомби над скоростью заражения или вывода из строя нормальных узлов.

С использованием разработанного экспериментального макета систем умного города проведено моделирование развития компьютерных атак типа «эксплуатация уязвимости ПО», «распределенный отказ в обслуживании», «черная дыра» и «атака большинства» в сети транспортных средств VANET и противодействия им различных комбинаций защитных механизмов. Экспериментальная верификация модели на макете подтвердила ее применимость для анализа атак различных типов. Разработанная модель позволяет в динамике определять оптимальную конфигурацию системы защиты для конкретных условий эксплуатации и обеспечивать устойчивость систем умного города к компьютерным атакам. При этом продемонстрировано, что комбинация методов машинного обучения, роевых алгоритмов и механизмов консенсуса обеспечивает высокую эффективность защиты, что критически важно для обеспечения устойчивости инфраструктуры умного города в условиях постоянно меняющегося ландшафта угроз.

План дальнейших исследований включает изучение масштабируемости предложенной модели оценки в условиях сверхбольших сетей и разработку среды тестирования защитных систем в условиях неопределенности и частичной наблюдаемости угроз.

Литература

1. Oliha J.S., Biu P.W., Obi O.C. Securing the Smart City: A Review of Cybersecurity Challenges and Strategies // Engineering Science and Technology Journal. 2024. vol. 5. no. 2. pp. 496–506.

2. Pavao J., Bastardo R., Rocha N.P. Cyber Resilience and Smart Cities, a Scoping Review // 18th Iberian Conference on Information Systems and Technologies (CISTI). 2023. pp. 1-6.
3. Romani G.F., Pinochet L.H.C., Pardim V.I., de Souza C.A. Security as a key factor for the smart city, citizens' trust, and the use of technologies // Revista de Administracao Publica. 2023. vol. 57. no. 2.
4. European Commission. Welcome to 2030: The Mega-trends. URL: https://ec.europa.eu/assets/epsc/pages/espas/chapter1.html (дата обращения: 26.06.2025).
5. Tushkanova O., Levshun D., Branitskiy A., Fedorchenko E., Novikova E., Kotenko I. Detection of Cyberattacks and Anomalies in Cyber-Physical Systems: Approaches, Data Sources, Evaluation // Algorithms. 2023. vol. 16. no. 2.
6. Петренко А.А., Петренко С.А. Технологии обеспечения киберустойчивости // Защита информации. Инсайд. 2021. № 6(102). С. 13–19.
7. AlSelami F.A. On the Implementation and Development of Smart Cities based on IoT Technology // International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies. 2021. vol. 12(7). pp. 1–12. DOI: 10.14456/ITJEMAST.2021.144.
8. Ullah A., Anwar S.M., Li J., Nadeem L., Mahmood T., Rehman A., Saba T. Smart cities: The role of Internet of Things and machine learning in realizing a data-centric smart environment // Complex and Intelligent Systems. 2024. vol. 10. pp. 1607–1637.
9. Ismagilova E., Hughes L., Rana N.P., Dwivedi Y.K. Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework // Information Systems Frontiers. 2022. vol. 24. pp. 393–414. DOI: 10.1007/s10796-020-10044-1.
10. Sharma S., Mishra N. Horizoning recent trends in the security of smart cities: Exploratory analysis using latent semantic analysis // Journal of Intelligent and Fuzzy Systems. 2024. vol. 46. pp. 579–596.
11. Павленко Е.Ю. Исследование влияния атак на структурные и параметрические метрики сетей с адаптивной топологией // Вопросы кибербезопасности. 2023. № 4(56). С. 65–71.
12. Waseem Anwar R., Ali S. Smart Cities Security Threat Landscape: A Review // Computing and Informatics. 2022. vol. 41. pp. 405–423.
13. Kwon H.J., Salim M.M., Park J.H. Recent Trends on Smart City Security: A Comprehensive Overview // Journal of Information Processing Systems. 2023. vol. 19(1). pp. 118–129. DOI: 10.3745/JIPS.03.0182.
14. Telo J. Smart City Security Threats and Countermeasures in the Context of Emerging Technologies // Journal of Intelligent Automation and Computing. 2023. vol. 6. no. 1. pp. 31–45.
15. Люльченко А.Н. Экспертная система оценки эффективности защиты информации // Защита информации. INSIDE. 2016. № 4. С. 20–24.
16. Евдокимов О.Г., Гавдан Г.П., Резниченко С.А. Подход к оценке эффективности системы обеспечения информационной безопасности распределенной системы передачи данных // Безопасность информационных технологий. 2022. Т. 29. № 2. С. 57–70.
17. Анисимов Е.Г., Анисимов В.Г., Гарькушев А.Ю., Селиванов А.А. Показатели эффективности межведомственного информационного взаимодействия при управлении обороной государства // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2016. № 7-8(97-98). С. 12–16.
18. Дровникова И.Г., Мещерякова Т.В., Попов А.Д., Рогозин Е.А., Ситник С.М. Математическая модель оценки эффективности систем защиты информации с

использованием преобразования Лапласа и численного метода Гивенса // Труды СПИИРАН. 2017. № 3(52). С. 234–258. DOI: 10.15622/sp.52.11.
19. Боровков В.Е., Ключарёв П.Г., Денисенко Д.И. Методика оценивания результативности функционирования систем обнаружения веб-бэкдоров // Информатика и автоматизация. 2025. Т. 24. № 1. С. 125–162. DOI: 10.15622/ia.24.1.6.
20. Бокова О.И., Дровникова И.Г., Етеппев А.С., Рогозин Е.А., Хвостов В.А. Методики оценивания надежности систем защиты информации от несанкционированного доступа в автоматизированных системах // Труды СПИИРАН. 2019. Т. 18. № 6. С. 1301–1332. DOI: 10.15622/sp.2019.18.6.1301-1332.
21. Трапезников Е.В. Алгоритм модели оценки защищенности информационной системы на основе нейронной сети // Известия Тульского государственного университета. Технические науки. 2017. № 2. С. 312–318.
22. Zhang L., Liu Y. Network Security Prediction and Situational Assessment Using Neural Network-based Method // Journal of Cyber Security and Mobility. 2023. vol. 12. no. 4. pp. 547–568. DOI: 10.13052/jcsm2245-1439.1245.
23. Авдошин А.С. Оценка защищенности информационной системы методами нечеткой логики // Вестник Самарского государственного технического университета. Серия: Технические науки. 2005. № 32. С. 191–193.
24. Миняев А.А., Красов А.В. Методика оценки эффективности системы защиты информации территориально-распределенных информационных систем // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 3. С. 26–32.
25. Atlam H.F., Walters R.J., Wills G.B., Daniel J. Fuzzy Logic with Expert Judgment to Implement an Adaptive Risk-Based Access Control Model for IoT // Mobile Networks and Applications. 2021. vol. 26. pp. 2545–2557. DOI: 10.1007/s11036-019-01214-w.
26. Космачева И.М., Давидюк Н.В., Сибикина И.В., Кучин И.Ю. Модель оценки эффективности конфигурации системы защиты информации на базе генетических алгоритмов // Моделирование, оптимизация и информационные технологии. 2020. Т. 8. № 3. DOI: 10.26102/2310-6018/2020.30.3.022.
27. Котенко И.В., Паращук И.Б. Особенности оперативной оценки защищенности критически важных ресурсов на основе адаптивной нейросетевой фильтрации // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2023. № 3. С. 55–64.
28. Котенко И.В., Степашкин М.В., Котенко Д.И., Дойникова Е.В. Оценивание защищенности информационных систем на основе построения деревьев социоинженерных атак // Известия высших учебных заведений. Приборостроение. 2011. Т. 54. № 12. С. 5–9.
29. Исмагилова А.С., Шагапов И.А., Салов И.В. Теоретико-графовая интерпретация системы защиты информации // Инженерный вестник Дона. 2024. № 9. С. 171–179.
30. Козленко А.В., Авраменко В.С., Саенко И.Б., Кий А.В. Метод оценки уровня защиты информации от НСД в компьютерных сетях на основе графа защищенности // Труды СПИИРАН. 2012. № 2(21). С. 41–55. DOI: 10.15622/sp.21.3.
31. Язов Ю.К., Авсентьев О.С., Рубцова И.О. К вопросу об оценке эффективности защиты информации в системах электронного документооборота // Вопросы кибербезопасности. 2019. № 1(29). С. 25–34.
32. Горохова В.Ф. Оптимизация выбора средств защиты от атак с использованием поглощающих марковских цепей // Материалы IV Всероссийской научно-

практической конференции с международным участием «Системы управления, информационные технологии и математическое моделирование». Омский государственный технический университет, 2022. С. 126–134.
33. Колмогоров А.Н. Качественное изучение математических моделей динамики популяций. // Проблемы кибернетики. 1972. Т. 5. № 2. С. 101–106.
34. Базыкин А.Д. Математическая биофизика взаимодействующих популяций // Академия наук СССР, Научно-исследовательский вычислительный центр. М.: Наука, 1985. 181 с.
35. Титов В.А., Вейнберг Р.Р. Анализ существующих динамических моделей на базе системы уравнений Лотки-Вольтерры «хищник-жертва» // Фундаментальные исследования. 2016. № 8-2. С. 409–413.
36. Братусь А.С., Новожилов А.С., Платонов А.П. Динамические системы и модели биологии // М.: Физматлит, 2011. 400 с.
37. Романов М.Ф., Федоров М.П. Математические модели в экологии: Учеб. пособие // СПб.: Иван Федоров, 2003. 239 с.
38. Вольтерра В. Математическая теория борьбы за существование // М.-Ижевск: Институт компьютерных исследований, 2004. 288 с.
39. Братусь А.С., Мещерин А.С., Новожилов А.С. Математические модели взаимодействия загрязнения с окружающей средой // Вестник МГУ. Серия «Вычислительная математика и кибернетика». 2001. Т. 6.
40. Марчук Г.И. Математические модели в иммунологии и медицине // М.: Наука, 1985.
41. Минаев В.А., Сычев М.П., Вайц Е.В., Грачева Ю.В. Математическая модель «хищник-жертва» в системе информационной безопасности // Информация и безопасность. 2016. Т. 19. № 3. С. 397–400.
42. Kamis N.H., Yassin W., Abdollah M.F., Razak S.F.A., Yogarayan S. Blackhole attacks in internet of things networks: a review // Indonesian Journal of Electrical Engineering and Computer Science. 2023. vol. 30. pp. 1080–1090.
43. Aponte-Novoa F.A., Orozco A.L.S., Villanueva-Polanco R., Wightman P. The 51% Attack on Blockchains: A Mining Behavior Study // IEEE Access. 2021. vol. 9. pp. 140549–140564.
44. Kalinin M., Krundyshev V. Security intrusion detection using quantum machine learning techniques // Journal of Computer Virology and Hacking Techniques. 2023. vol. 19. no. 1. pp. 125–136.
45. Krundyshev V., Kalinin M., Zegzhda P. Artificial swarm algorithm for VANET protection against routing attacks // IEEE Industrial Cyber-Physical Systems (ICPS). 2018. pp. 795–800.
46. Васильев О.С., Крундышев В.М. Защита систем распределенного реестра умного города на основе модели доверия // Материалы 34-й научно-технической всероссийской конференции «Методы и технические средства обеспечения безопасности информации». СПб: Изд-во Политехнического университета, 2025. С. 109–110.

Крундышев Василий Михайлович — канд. техн. наук, доцент, институт компьютерных наук и кибербезопасности, Санкт-Петербургский политехнический университет Петра Великого. Область научных интересов: методы искусственного интеллекта для компьютерной безопасности, модели безопасности, оценка безопасности. Число научных публикаций — 120. vmk@ibks.spbstu.ru; Политехническая улица, 29, 195251, Санкт-Петербург, Россия; р.т.: +7(812)552-7632.

Калинин Максим Олегович — д-р техн. наук, профессор, институт компьютерных наук и кибербезопасности, Санкт-Петербургский политехнический университет Петра

Великого. Область научных интересов: анализ киберрисков, машинное обучение для кибербезопасности, киберустойчивость, модели безопасности киберфизических систем. Число научных публикаций — 320. max@ibks.spbstu.ru; Политехническая улица, 29, 195251, Санкт-Петербург, Россия; р.т.: +7(812)552-7632.

Поддержка исследований. Исследование выполнено за счет гранта Российского научного фонда № 24-11-20005, https://rscf.ru/project/24-11-20005/, грант Санкт-Петербургского научного фонда (договор № 24-11-20005 о предоставлении регионального гранта).

DOI 10.15622/ia.25.1.3

V. KRUNDYSHEV, M. KALININ

EVALUATION OF INFORMATION SECURITY EFFICIENCY IN SMART CITY SYSTEMS BASED ON A COMPETITION MODEL

Krundyshev V., Kalinin M. **Evaluation of Information Security Efficiency in Smart City Systems Based on a Competition Model.**

Abstract. The implementation of the smart city concept implies a transition from traditional computer networks with a clear information perimeter to next-generation networks. Distributed subsystems of a smart city are characterized by a reconfigurable network topology, openness, node mobility, and the construction of information protection based on distributed ledgers, which also opens up new opportunities for intruders. The situation is complicated by the fact that the speed of creating new digital infrastructures exceeds the speed of developing security tools that meet current challenges. Given the specific properties of the secured object, the dynamics of security threats, and the limited choice of security mechanisms, it is necessary to continuously evaluate the security efficiency and reconfigure it to maintain a higher level of security. As a result of the analysis of existing solutions for information security evaluation, it was found that they operate in a proactive mode and do not take into account the high dynamics of the "threat-protection" system. This paper presents a constructed model for evaluating the efficiency of information security, based on a nonlinear dynamic model of competition for influence on the functioning of the information infrastructure. To maintain a sustainable state of the smart city system, it is necessary to meet the criterion on the ratio of the speed of detection and development of a computer attack in the infrastructure. The developed experimental model emulated the scenarios of development of computer attacks "exploitation of software vulnerability", "distributed denial of service", "black hole", and "majority attack" using the test sample of the intelligent transport network VANET in the smart city in various configurations of the security system. During the comparative analysis of different configurations of the VANET security system, it was shown that a test case implementing attack detection using a convolutional neural network, dynamic routing based on the ant swarm algorithm, and the Hashgraph protocol with an embedded trust model satisfies the sustainability criterion. The use of the proposed evaluation model allows for reasonable control and dynamic adjustment of the security configuration.

Keywords: distributed ledger, sustainability criterion, competition model, efficiency assessment, speed of computer attack, sustainability point, smart city.

References

1. Oliha J.S., Biu P.W., Obi O.C. Securing the Smart City: A Review of Cybersecurity Challenges and Strategies. Engineering Science and Technology Journal. 2024. vol. 5. no. 2. pp. 496–506.
2. Pavao J., Bastardo R., Rocha N.P. Cyber Resilience and Smart Cities, a Scoping Review. 18th Iberian Conference on Information Systems and Technologies (CISTI). 2023. pp. 1-6.
3. Romani G.F., Pinochet L.H.C., Pardim V.I., de Souza C.A. Security as a key factor for the smart city, citizens' trust, and the use of technologies. Revista de Administracao Publica. 2023. vol. 57. no. 2.
4. European Commission. Welcome to 2030: The Mega-trends. Available at: https://ec.europa.eu/assets/epsc/pages/espas/chapter1.html (accessed 26.06.2025).

5. Tushkanova O., Levshun D., Branitskiy A., Fedorchenko E., Novikova E., Kotenko I. Detection of Cyberattacks and Anomalies in Cyber-Physical Systems: Approaches, Data Sources, Evaluation. Algorithms. 2023. vol. 16. no. 2.
6. Petrenko A.A., Petrenko S.A. [Cyber Resilience Technologies]. Zashhita Informacii. Insajd – Information Security. Inside. 2021. no. 6(102). pp. 13–19. (In Russ.).
7. AlSelami F.A. On the Implementation and Development of Smart Cities based on IoT Technology. International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies. 2021. vol. 12(7). pp. 1–12. DOI: 10.14456/ITJEMAST.2021.144.
8. Ullah A., Anwar S.M., Li J., Nadeem L., Mahmood T., Rehman A., Saba T. Smart cities: The role of Internet of Things and machine learning in realizing a data-centric smart environment. Complex and Intelligent Systems. 2024. vol. 10. pp. 1607–1637.
9. Ismagilova E., Hughes L., Rana N.P., Dwivedi Y.K. Security, Privacy and Risks within Smart Cities: Literature Review and Development of a Smart City Interaction Framework. Information Systems Frontiers. 2022. vol. 24. pp. 393–414. DOI: 10.1007/s10796-020-10044-1.
10. Sharma S., Mishra N. Horizoning recent trends in the security of smart cities: Exploratory analysis using latent semantic analysis. Journal of Intelligent and Fuzzy Systems. 2024. vol. 46. pp. 579–596.
11. Pavlenko E.Yu. [Study of the Impact of Attacks on Structural and Parametric Metrics of Networks with Adaptive Topology]. Voprosy kiberbezopasnosti – Cybersecurity Issues. 2023. no. 4(56). pp. 65–71. (In Russ.).
12. Waseem Anwar R., Ali S. Smart Cities Security Threat Landscape: A Review. Computing and Informatics. 2022. vol. 41. pp. 405–423.
13. Kwon H.J., Salim M.M., Park J.H. Recent Trends on Smart City Security: A Comprehensive Overview. Journal of Information Processing Systems. 2023. vol. 19(1). pp. 118–129. DOI: 10.3745/JIPS.03.0182.
14. Telo J. Smart City Security Threats and Countermeasures in the Context of Emerging Technologies. Journal of Intelligent Automation and Computing. 2023. vol. 6. no. 1. pp. 31–45.
15. Ljul'chenko A.N. [Expert system for assessing the effectiveness of information security]. Zashhita Informacii. Insajd – Information Security. Inside. 2016. no. 4. pp. 20–24. (In Russ.).
16. Evdokimov O.G., Gavdan G.P., Reznichenko S.A. [An approach to assessing the effectiveness of the information security system of a distributed data transmission system]. Bezopasnost' informacionnyh tehnologij – Information Technology Security. 2022. vol. 29. no. 2. pp. 57–70. (In Russ.).
17. Anisimov E.G., Anisimov V.G., Gar'kushev A.Ju., Selivanov A.A. [Performance indicators of interdepartmental information interaction in the management of national defense]. Voprosy oboronnoj tehniki. Serija 16: Tehnicheskie sredstva protivodejstvija terrorizmu – Defense Technology Issues. Series 16: Technical Counterterrorism Equipment. 2016. no. 7-8(97-98). pp. 12–16. (In Russ.).
18. Drovnikova I., Meshherjakova T., Popov A., Rogozin E., Sitnik S. [Mathematical model for estimating the efficiency of information security systems by means of Laplace transformation and Givens method]. SPIIRAS Proceedings. 2017. vol. 52. no. 3. pp. 234–258. DOI: 10.15622/sp.52.11. (In Russ.).
19. Borovkov V.E., Kljucharev P.G., Denisenko D.I. [Methodology for assessing the performance of web backdoor detection systems]. Informatics and automation. 2025. vol. 24. no. 1. pp. 125–162. DOI: 10.15622/ia.24.1.6. (In Russ.).
20. Bokova O.I., Drovnikova I.G., Etepnev A.S., Rogozin E.A., Hvostov V.A. [Methods for assessing the reliability of information protection systems against unauthorized

access in automated systems]. SPIIRAS Proceedings. 2019. vol. 18. no. 6. pp. 1301–1332. DOI: 10.15622/sp.2019.18.6.1301-1332. (In Russ.).
21. Trapeznikov E.V. [Algorithm for assessing the security of an information system based on a neural network]. Izvestija Tul'skogo gosudarstvennogo universiteta. Tehnicheskie nauki – News of Tula State University. Technical Sciences. 2017. no. 2. pp. 312–318. (In Russ.).
22. Zhang L., Liu Y. Network Security Prediction and Situational Assessment Using Neural Network-based Method. Journal of Cyber Security and Mobility. 2023. vol. 12. no. 4. pp. 547–568. DOI: 10.13052/jcsm2245-1439.1245.
23. Avdoshin A.S. [Evaluation of information system security using fuzzy logic methods]. Vestnik Samarskogo gosudarstvennogo tehnicheskogo universiteta. Serija: Tehnicheskie nauki – Bulletin of Samara State Technical University. Series: Technical Sciences. 2005. no. 32. pp. 191–193. (In Russ.).
24. Minjaev A.A., Krasov A.V. [Methodology for assessing the effectiveness of the information security system of geographically distributed information systems]. Vestnik Sankt-Peterburgskogo gosudarstvennogo universiteta tehnologii i dizajna. Serija 1: Estestvennye i tehnicheskie nauki – Bulletin of the Saint Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. 2020. no. 3. pp. 26–32. (In Russ.).
25. Atlam H.F., Walters R.J., Wills G.B., Daniel J. Fuzzy Logic with Expert Judgment to Implement an Adaptive Risk-Based Access Control Model for IoT. Mobile Networks and Applications. 2021. vol. 26. pp. 2545–2557. DOI: 10.1007/s11036-019-01214-w.
26. Kosmacheva I.M., Davidjuk N.V., Sibikina I.V., Kuchin I.Ju. [Model for assessing the efficiency of information security system configuration based on genetic algorithms]. Modelirovanie, optimizacija i informacionnye tehnologii – Modeling, optimization and information technologies. 2020. vol. 8. no. 3. DOI: 10.26102/2310-6018/2020.30.3.022. (In Russ.).
27. Kotenko I.V., Parashhuk I.B. [Features of operational assessment of the security of critical resources based on adaptive neural network filtering]. Vestnik Astrahanskogo gosudarstvennogo tehnicheskogo universiteta. Serija: Upravlenie, vychislitel'naja tehnika i informatika – Bulletin of the Astrakhan State Technical University. Series: Control, Computer Technics and Informatics. 2023. no. 3. pp. 55–64. (In Russ.).
28. Kotenko I.V., Stepashkin M.V., Kotenko D.I., Dojnikova E.V. [Evaluation of the security of information systems based on the construction of trees of social engineering attacks]. Izvestija vysshih uchebnyh zavedenij. Priborostroenie – News of higher educational institutions. Instrument engineering. 2011. vol. 54. no. 12. pp. 5–9. (In Russ.).
29. Ismagilova A.S., Shagapov I.A., Salov I.V. [Graph-theoretic interpretation of information security system]. Inzhenernyj vestnik Dona – Engineering Bulletin of the Don. 2024. no. 9. pp. 171–179. (In Russ.).
30. Kozlenko A.V., Avramenko V.S., Saenko I.B., Kij A.V. [Method of assessing the level of information protection against unauthorized access in computer networks on the basis of the security graph]. SPIIRAS Proceedings. 2012. vol. 21. no. 2. pp. 41–55. DOI: 10.15622/sp.21.3. (In Russ.).
31. Jazov Ju.K., Avsent'ev O.S., Rubcova I.O. [On the issue of assessing the effectiveness of information protection in electronic document management systems]. Voprosy kiberbezopasnosti – Cybersecurity Issues. 2019. no. 1(29). pp. 25–34. (In Russ.).
32. Gorohova V.F. [Optimizing the Choice of Defenses against Attacks Using Absorbing Markov Chains]. Materialy IV Vserossijskoj nauchno-prakticheskoj konferencii s mezhdunarodnym uchastiem. Omskij gosudarstvennyj tehnicheskij universitet «Sistemy upravlenija, informacionnye tehnologii i matematicheskoe modelirovanie» [Proceedings of the IV All-Russian scientific-practical conference with international

participation. Omsk State Technical University «Control systems, information technologies and mathematical modeling»]. 2022. pp. 126–134. (In Russ.).
33. Kolmogorov A.N. [Qualitative study of mathematical models of population dynamics]. Problemy kibernetiki – Problems of cybernetics. 1972. vol. 5. no. 2. pp. 101–106. (In Russ.).
34. Bazykin A.D. Matematicheskaja biofizika vzaimodejstvujushhih populjacij [Mathematical biophysics of interacting populations]. USSR Academy of Sciences, Research Computing Center. Moscow: Nauka, 1985. 181 p. (In Russ.).
35. Titov V.A., Vejnberg R.R. [Analysis of existing dynamic models based on the Lotka-Volterra predator-prey equation system]. Fundamental'nye issledovanija – Fundamental research. 2016. no. 8-2. pp. 409–413. (In Russ.).
36. Bratus' A.S., Novozhilov A.S., Platonov A.P. Dinamicheskie sistemy i modeli biologii [Dynamic systems and models of biology]. Moscow: Fizmatlit, 2011. 400 p. (In Russ.).
37. Romanov M.F., Fedorov M.P. Matematicheskie modeli v jekologii : Uchebnoe posobie [Mathematical models in ecology: Tutorial]. St. Petersburg: Ivan Fedorov, 2003. 239 p. (In Russ.).
38. Volterra V. Matematicheskaja teorija bor'by za sushhestvovanie [Mathematical theory of the struggle for existence]. Moscow-Izhevsk: Institute of Computer Research, 2004. 288 p. (In Russ.).
39. Bratus' A.S., Meshherin A.S., Novozhilov A.S. [Mathematical models of the interaction of pollution with the environment]. Vestnik MGU. Serija «Vychislitel'naja matematika i kibernetika» – Moscow State University Bulletin. Series "Computational Mathematics and Cybernetics". 2001. vol. 6. (In Russ.).
40. Marchuk G.I. Matematicheskie modeli v immunologii i medicine [Mathematical models in immunology and medicine]. Moscow: Nauka, 1985. (In Russ.).
41. Minaev V.A., Sychev M.P., Vajc E.V., Gracheva Ju.V. [Mathematical model of "predator-prey" in the information security system]. Informacija i bezopasnost' – Information and Security. 2016. vol. 19. no. 3. pp. 397–400. (In Russ.).
42. Kamis N.H., Yassin W., Abdollah M.F., Razak S.F.A., Yogarayan S. Blackhole attacks in internet of things networks: a review. Indonesian Journal of Electrical Engineering and Computer Science. 2023. vol. 30. pp. 1080–1090.
43. Aponte-Novoa F.A., Orozco A.L.S., Villanueva-Polanco R., Wightman P. The 51% Attack on Blockchains: A Mining Behavior Study. IEEE Access. 2021. vol. 9. pp. 140549–140564.
44. Kalinin M., Krundyshev V. Security intrusion detection using quantum machine learning techniques. Journal of Computer Virology and Hacking Techniques. 2023. vol. 19. no. 1. pp. 125–136.
45. Krundyshev V., Kalinin M., Zegzhda P. Artificial swarm algorithm for VANET protection against routing attacks. IEEE Industrial Cyber-Physical Systems (ICPS). 2018. pp. 795–800.
46. Vasil'ev O.S., Krundyshev V.M. [Securing Smart City Distributed Ledger Systems Based on a Trust Model] Materialy 34-j nauchno-tehnicheskoj vserossijskoj konferencii «Metody i tehnicheskie sredstva obespechenija bezopasnosti informacii» [Proceedings of the 34th Scientific and Technical All-Russian Conference «Methods and technical means of ensuring information security»]. 2025. pp. 109–110. (In Russ.).

Krundyshev Vasiliy — Ph.D., Associate Professor, Institute of computer science and cybersecurity, Peter the Great St. Petersburg Polytechnic University. Research interests: methods of artificial intelligence for computer security, security models, security evaluation. The number of publications — 120. vmk@ibks.spbstu.ru; 29, Politekhnicheskaya St., 195251, St. Petersburg, Russia; office phone: +7(812)552-7632.

Kalinin Maxim — Ph.D., Dr.Sci., Professor, Institute of computer science and cybersecurity, Peter the Great St. Petersburg Polytechnic University. Research interests: cyber risk analysis, machine learning for cybersecurity, cyber resiliency, models for cyber-physical system protection. The number of publications — 320. max@ibks.spbstu.ru; 29, Politekhnicheskaya St., 195251, St. Petersburg, Russia; office phone: +7(812)552-7632.

Acknowledgements. The study was supported by a grant from the Russian Science Foundation No. 24-11-20005, https://rscf.ru/project/24-11-20005/; grant of St. Petersburg Science Foundation (Agreement No. 24-11-20005 on the regional grant).